Data Security Manual

MANILA BANKERS
LIFE INSURANCE CORPORATION

Foreword

Gentlemen:
In the age of continuous connection, we offer our customers the freedom and convenience to transact online. This requires data to be collected and processed. When processing, storing and transmitting data, we must ensure a high level of data protection and data security. This standard must be in place for all the subjects we deal whether they be our brokers/agents, employees, clients, or industry partners.

For this purpose, we must set the standard in data protection. It is our duty as a member of the insurance industry to comply with Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012, the rules and regulations of the National Privacy Commission because protecting the personal rights and privacy of each data subject has become the foundation of trust in our business relationships.

Our Data Security Manual lays down the obligations of each member of the organization for processing personal data pertaining to customers, prospects, business partners and employees. It meets the standards set forth in the Data Privacy Act. The policy sets applicable data protection and security standard for our company and regulates the sharing of information between our group companies. We have established our data protection policies, among them are those prescribed by the National Privacy Commission – transparency, legitimacy, and proportionality.

Our managers and employees are obligated to adhere to the requirements set forth in this Data Security Manual. As the Data Protection Officer, it is my duty to ensure that the rules and principles of data protection and security at Manila Bankers are followed with a high sense of accountability and confidentiality.

I will be pleased to answer any questions you have about data protection and security at Manila Bankers.

Gabriela E. Calma-Chan
Data Protection Officer

Contents

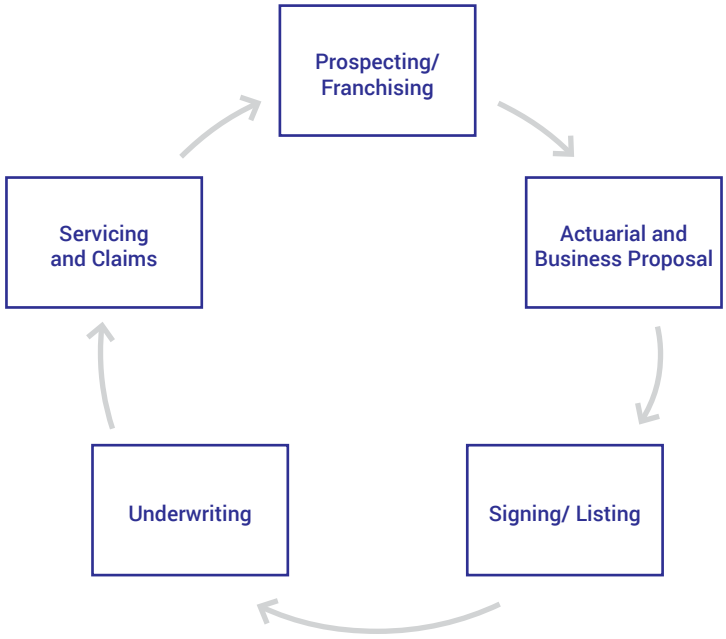
I.
Aim of the Data Protection Policy

Manila Bankers Life Insurance Corporation (Manila Bankers) is committed to the policy and mandate of the government to protect the fundamental human right of privacy and communication while ensuring the free flow of information to promote innovation, growth, and efficiency.

Moving forward in this digital age, we cannot deny the vital role of information and communications technology in business and in day-to-day affairs and with this, the inherent obligation to ensure personal information in information and communications systems are always protected.

II.
Processing of Personal Data

Manila Bankers Life has organized and streamlined the systems and processes involving personal data. A list of the processes of MBLife are summarized in the Data Life Cycle under Figure 12. Below is the Data Life Cycle:



1. COLLECTION

It is the mandate of the Board of MBLife that all personal data collected must be with consent and for a legitimate purpose. Consent should be secured prior to collection and processing of personal data. In the event that personal information was obtained prior to securing the consent of the data subject, it is the responsibility of the employee of MBLife creating or collecting personal data to secure consent, within a reasonable time after obtaining the personal information. Consent must be express and informed. It may be given in any form, oral or written, in which case it is the obligation of the employee to document the consent given.
See Policy for Privacy Notice

If the data subject should withhold his/her consent, it is the responsibility of the employee to update the records of MBLife and delete the information of the data subject from all the records of the MBLife and coordinate with the Information Technology (IT) Team to put the data subject in the DNC list. See Policy for DNC

Guidelines

- Consent is required prior to collection or, exclusively for personal information, within a reasonable time after collection of the personal information
- The Data subject must be provided with specific information regarding the purpose and extent of processing
- Only personal data that is necessary and consistent with declared, specified, and legitimate purpose shall be collected

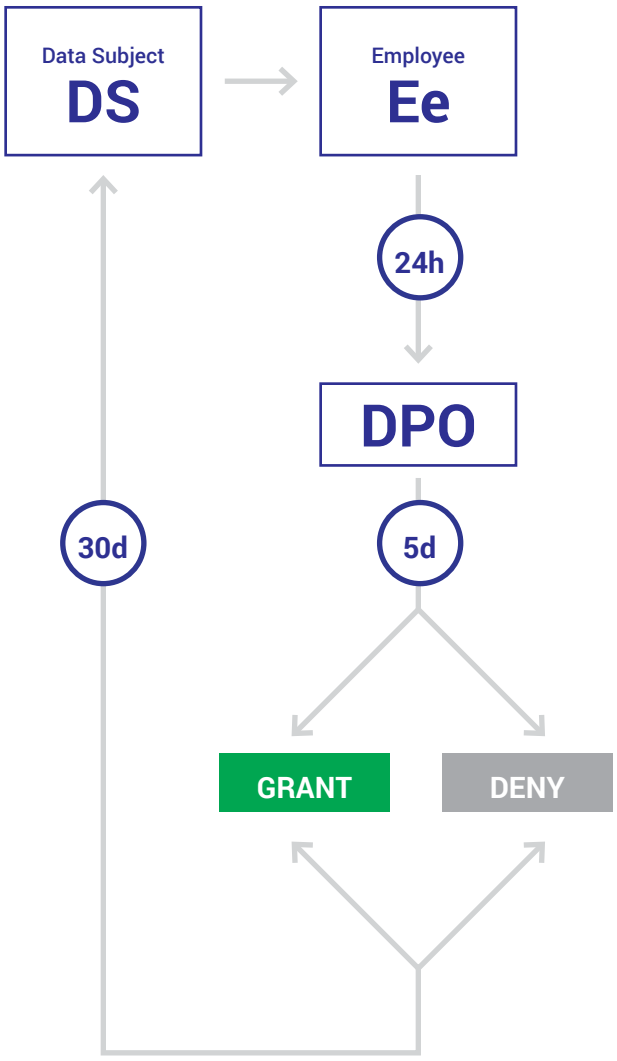
2. USE

When collecting and processing personal data, the rights of the data subject must always be protected. You may refer to the rights of the data subject in the Privacy Manual. If a data subject should make known his/her desire to exercise his/her rights, the employee must secure the following information from the data subject-

- Complete name
- Contact details
- Competent evidence of identification
- Letter stating the request of the data subject and the purpose of the request

Within twenty-four (24) hours from receipt, the employee must forward the request to the DPO. Upon referral to the DPO, the DPO shall have five (5) business days to assess the request of the data subject, depending on the circumstance, the DPO may grant or deny the same. The DPO must document the approval or denial thereof and the circumstances surrounding it.

A request for the exercise of the rights of the data subject shall not prevent MBLife from charging any fees or assessments which are necessarily included or related to the fulfillment of the request of the data subject.
In the exercise of the rights of the data subject. MBLife shall have a period of thirty (30) calendar days from submission of complete documents and referral to the DPO to comply with the request of the data subject, unless a longer period is required, in which case, the DPO shall inform the data subject within the thirty (30) day period that his/her request shall take more than the usual thirty (30) calendar days.



3. STORAGE

Data collected and processed by MBLife are stored manually and electronically. Hard copies of documents containing personal information are stored in a secure location 24/7 and may be accessed only upon filing an Access Request with the Admin Officer with approval from the DPO.

Information stored electronically are placed in a Data Center that houses the Server. It is the obligation of the IT Department to ensure that the Serves are secure at all times and only authorized personnel are granted access to them.

All members of MBLife have a duty of confidentiality and accountability to the data subjects. All personal data that is within their control must be properly secured and/or disposed. SEE Policy on Passwords and Security Codes.

4. ACCESS/DISCLOSURE

In order to protect personal data, only authorized persons shall have access to personal data. All computers, laptops, mobile phones, and other gadgets must, at all times, be protected by a password/access code. Upon issuance, a default password may be issued by IT. It is the responsibility of the member concerned to change the default passwords immediately. Furthermore, passwords or codes are strictly confidential and must never be disclosed to third parties. Disclosing of passwords or security codes shall be punishable.

Members of MBLife who must disclose personal data to third parties must ensure that prior to disclosing these information, they have executed an Outsourcing Agreement, a Non-Disclosure Agreement, or a Data Sharing Agreement, as the case may be in addition to the Principcal Contract.

5. DISPOSAL

MBLife, due to the nature of the business and consistent with the policies of the Insurance Commission, retains personal information 9 years after the death of an insured. This is to protect against redundant death claims. Depending on the type of document, the retention period will vary. For instance, for government documents, the retention period is 5 years. For this purpose, each department is tasked to establish, their own retention policies for personal data under them including disposal procedures upon the termination of the retention period.

All documents, whether stored manually or electronically, must be disposed of responsibly to prevent unauthorized disclosure or breach. When data is shared to third parties, the governing agreement must always contain a Proper Disposal Procedure with an assurance supported by a statement under oath that upon disposal, the receiving party shall execute a document attesting to the proper and certain disposal of personal data shared.

III.
Security Measures

The Data Privacy Act requires all Personal Information Controller to implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, and unlawful processing.

1. ORGANIZATION

1.1 Data Protection Officers

In addition to the Data Protection Officer, each department head or area head shall be Compliance Officers for Privacy who shall be responsible for implementing the Privacy Management Program and this Dat Security Manual in their team.

1.2 Functions

The Data Protections Officers shall be independent and autonomous. The following is a summary of the functions of the DPO-

- Monitor the compliance of the PIC
- Ensure the conduct of the Privacy Impact Assessments
- Ensure that the rights of the data subjects are protected
- Must ensure proper breach management
- Cultivate internal awareness on data privacy
- Advocate Privacy-by-Design
  SEE Policy on Privacy By Design
- Serve as the point person for privacy matters
- Serve as a conduit of the National Privacy Commission

The Compliance Officers for Privacy shall have the following functions-

- Must ensure proper breach management
- Cultivate internal awareness on data privacy
- Advocate Privacy-by-Design
- Serve as the point person for privacy matters
- Serve as a conduit of the National Privacy Commission

The DPO together with the Compliance Officers for Privacy shall work hand in hand in complying with the Data Privacy Act and in the conduct of the aforementioned duties and responsibilities.

1.3 Conduct of Training

All the members of MBLife shall undergo privacy training at least once a year. The Human Resources (HR) Department is responsible for documenting the conduct of training and shall ensure that all newly hired employees must first undergo a privacy seminar with the DPO. These may be made by a request through email.

In coordination with the Compliance Officers for Privacy and the HR Department, the DPO may initiate training other than an annual meeting, in the event that, in the opinion of the DPO, there is a need to discuss important regulations of the NPC or to apprise the members of MBLIfe regarding current news or events relevant to the insurance industry.

1.4 Conduct of Privacy Impact Assessment (PIA)

Notwithstanding the list under Figure 10, all new or revised programs, processes, measure, systems, technology (PPMST) must undergo a privacy impact assessment substantially in the form and substance as provided under Figure 11.

For new PPMSTs, the PPMST lead must coordinate with the DPO to implement the (SEE) Policy on Privacy by Design. Privacy by Design requires that privacy risks must first be assessed PRIOR TO any planned PPMST.

The PPMST owner shall prepare a management report substantially in the form under Figure 12 appraising management of recommendations and timelines. Results of the PIA shall be revisited every year or unless sooner necessary when there are revisions to the PPMST. The results of the PIA shall be documented and shall be ready for inspection upon request of the DPO or the Breach Management Team. The PPMST owner shall inform the DPO in the event of any changes.

1.5 Mandatory Training

The DPO is required to undergo mandatory training under the National Privacy Commission or its duly accredited training providers.

1.6 Duty of Confidentiality and Accountability

Consistent with the Data Protection Policies, all members of MBLife have a duty of confidentiality and accountability. Section 21 of DPA of 2012 states that-

> "each PIC is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestic or international, subject to cross border arrangement and cooperation."

For this purpose, all employees and members of MBLife shall be required to sign a Non-Disclosure Agreement. The DPO, in coordination with the HR Department, shall ensure this requirement is complied with at all times.

1.7 Review of Privacy Manual

This Privacy Manual shall be reviewed every year and shall be amended when in the opinion of the DPO, amendments are necessary to better protect the rights of the data subjects. All amendments to the privacy manual shall be with prior notice to the members of MBLife.

2. PHYSICAL

2.1 Format of Data Collected

Personal data collected by MBLife are stored either in electronic/digital formant and/or paper-based/ physical format.

2.2 Storage and Location

Physical data in the custody of MBLife are stored in a location offsite and manned by a security officer 24/7. Access to the location are restricted and all requests for access to physical data with MBLife are required to be supported by Access request forms, and approved by of the DPO.

Data stored in digital format are stored and located in the server, referred to the Data Center. Access to the data center is restricted and the server rooms are likewise protected by a security officer 24/7.

2.3 Access Procedures

Only authorized personnel are allowed access to data room and the data center. For the offsite data room containing physical data, the Admin Department shall be responsible for the security and access controls. For the data center, the IT Department shall be responsible for implementing the security and access controls. The Admin and IT Department shall register the names and contact details of all the authorized personnel who have access to the data room and the data center with the DPO. All requests for access shall be supported by filing an Access Request Form with the DPO. The DPO may grant or deny the request for access.

The Access Request Form shall have the following information-

- The name and contact details of the person requesting access
- The purpose and extent of the access
- The period of the access

When granted, the Admin or IT Department, as the case may be, shall ensure that an authorized personnel is always present during access by the concerned employee/member of MBLife.

2.4 Monitoring and Limiting of Access

All members of MBLife authorized to enter and access the data room or facility must fill out and register with the online registration platform of MBLife. A logbook shall also be placed at the entrance of the room. Each person granted access must indicate the following details in the logbook upon entry and exit.

- Data
- Time
- Duration
- Purpose

SEE Policy on Access Procedures

2.5 Working Space Design

The working space design shall be in attuned with the Privacy Manual of MBLife. Computers and office spaces shall have considerable space between them to maintain privacy and protect the processing of personal data. This shall also be applied to all branches of MBLife in malls and other areas where a data subject will fill up an application form. The concerned members of MBLife shall establish working space design guidelines to prevent unintended disclosures during the creation and collection of personal data.

2.6 Modes of Transfer

Transfers of personal data to third parties shall always be supported by a duly executed Non Disclosure Agreement, an Outsourcing Agreement for Privacy, or a Data Sharing Agreement, as the case may be. These forms are provided for as Annexes in the Data Protection Policies. You may also get in touch with the DPO for customized documents.

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data including all attachments. SEE Policy on Encryption Facsimile technology shall not be allowed for transmitting documents containing personal data.

2.7 Retention and Disposal

For insured clients, MBLife shall retain the personal data of the client for __ years upon the death of the data subject. For remorse client, the personal data of the data subject shall be uploaded in the Medical Information Database consistent with Insurance Commission (IC) Circular No. _____.

For employees of MBLife, MBLife shall retain the personal data of the employee for 1 year after separation from MBLife. For employee applicants, MBLife shall retain personal data for 30 days from selecting the hired applicant.

Upon expiration of the periods set forth herein, all physical and digital copies of the personal data shall be destroyed and disposed of using secure technology. The process owner shall execute an affidavit that all copies of the personal data have been disposed of securely. SEE Policy on Proper Disposal

3. TECHNICAL

3.1 Breach Monitoring

MBLife shall employ detection systems to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

3.2 Software Security Features

All members of MBLife are prohibited from installing or downloading software applications on computers and devices brought into the office and using the network of the organization. All software applications must be first reviewed, evaluated, and approved by the IT Department to ensure the compatibility of security features with overall operations. SEE Policy on Software Security

3.3 Process of Regular Testing and Assessment

MBLife, in coordination with the Data Breach Response Team, shall review security policies, conduct vulnerability assessments, and perform penetration testing within the organization at least twice a year.

All members of MBLife with access to personal data shall verify his/her identity using a secure encrypted link and multi-level authentication established by the IT Department in coordination with the Privacy Officers. SEE Policy on Passwords and Access Codes When a member is given an office issued computer or device, these shall be equipped with a username and default password. It is the responsibility of the member to immediately change the default password and keep this password confidential.

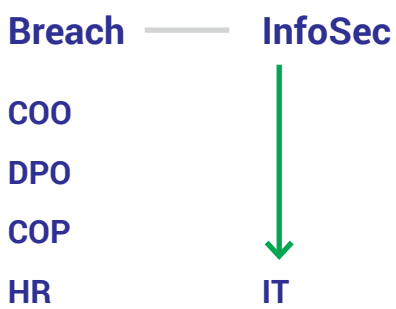
IV.
Breach Management Procedures

1. SECURITY INCIDENT POLICY

The Security Incident Policy of MBLife adheres to the standards of the security policy mandated by the NPC. The purpose of the this policy is to create measures to prevent, minimize, or manage the occurrence of a personal data breach.

The following measures are adopted by MBLife under their Security Incident Policy-

- The conduct of a Privacy Impact Assessment to prepare for attendant risks
- Data Governance Policy that ensures adherence to transparency, legitimate purpose, and proportionality when collecting and processing personal data
- Implementation of Security Measures as evolved through the conduct of PIAs
- Regular monitoring of security breaches through the IT department and responsible Compliance Officers for Privacy
- Capacity Building of personnel through mandatory trainings and seminars to ensure knowledge of data breach management principles and internal procedures for reporting security incidents
- Procedure for regular review of policies and procedures



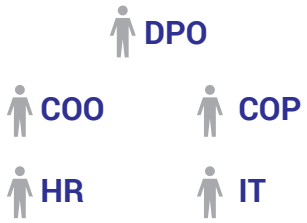
2. DATA BREACH RESPONSE TEAM

The Data Breach Response Team is responsible for the following-

- Implementing security incident management policy of MBLife
- Managing security incidents and personal data breaches
- Compliance with the relevant provisions of Republic Act No. 10173, its IRR, and related issuances by the NPC on personal data breach management

3. INCIDENT RESPONSE TEAM

The incident response team shall be composed of the Chief Operations Officer, DPO, the Compliance Officer, and the HR Manager.



In cases where the incident involves a breach in information communication systems, the IT Head shall be part of the Incident Response Team.

All security incidents or threatened security incidents shall be immediately reported to the DPO directly who shall then convene the Incident Response Team within 24h. The Incident Response Team shall meet and assess the security incident. Upon assessment, the Incident Response Team take immediate decision regarding critical action.

4. BREACH DOCUMENTATION

The Incident Response Team shall be responsible for documenting the Security Incident and reporting them to the NPC, where applicable. Breach documentation shall include-

- The facts surrounding the incident
- The effects of such incident
- The remedial action taken by the Incident Response Team
- Outcome of breach management and difficulties encountered
- Compliance with notification requirements and assistance provided to the affected data subject, where applicable
- Such other information available to document the security incident

Included in the documentation of the breach are proposed remedial measures to prevent or mitigate the breach and a call to action to conduct a Privacy Impact Assessment on the process involved in the breach.

5. BREACH NOTIFICATION

Security Incidents shall be reported to the NPC annually substantially in the form provided by the NPC under Advisory No. 18-02.

The annual report to the NPC shall also state a summary of the security incidents for the year including information such as the number of security incidents and breach encountered and the information compromised classified according to their impact on availability, integrity, or confidentiality of personal data.

In cases of Personal Data Breach Requiring Notification, the Incident Response Team, upon determination as such, shall report the breach to the NPC within 72 hours upon knowledge or reasonable belief by MBLIfe that a security breach requiring notification has occurred except where delay is caused by the determination of the scope of the breach, made to prevent further disclosures, made to restore the integrity of the information and communications system. In all cases, the notification shall state the following-

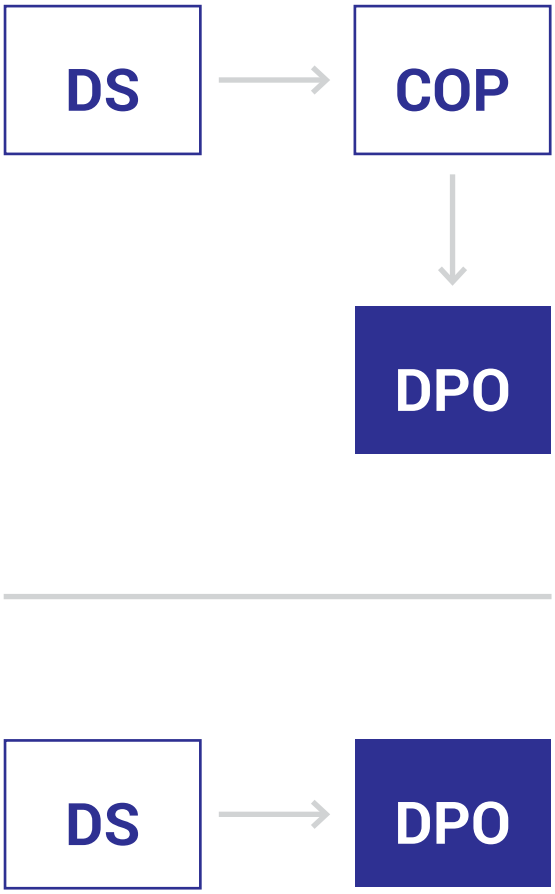
- The nature of the breach describing the events as it unfolded and an estimate of the number of data subjects affected
- A statement of the personal data involved
- Remedial measures taken by MBLife
- The name and contact information of the DPO

V.
Inquiries and Complaints

All inquiries and complaints shall first be relayed to the department head acting as the Compliance Officer for Privacy. The COP shall thereafter refer the inquiry or complaint to the DPO who shall assess the inquiry and complaint and act according to the DPA of MBLife.

In the event that a complaint affects personal data, the complaint shall be referred to the DPO directly without going through the COP. It shall be the responsibility of the DPO to inform the COP within a practicable time after mitigating the breach issue.

A data subject may be a client, a potential client, an agent, or an employee of MBLife. In all cases, the foregoing procedure shall be followed and the procedure for the exercise of the rights of the data subject shall apply suppletorily.



VI.
Penalties

A violation of any of the Policies on Privacy, Breach, and Security shall, depending on the severity, be punishable from Written Warning to Dismissal. The imposition of Dismissal is due to the gravity of the possible consequences of personal data breach and in keeping with the provisions of the Data Privacy Act which provides imprisonment as penalty. Likewise, a commission of any of the offenses under Section 25 to 35 of the DPA shall likewise be punishable from Written Warning to Dismissal. SEE Summary of Offenses under FIGURE 13

PENALTY	LEVELS OF APPROVING AUTHORITY
6.1 Written Warning (W) - a reprimand given to an employee who has committed a violation, usually for the first time. It is given to an employee for minor offenses. All items discussed shall be documented through a Performance Improvement Plan ("PIP").	Immediate Superior and noted by the Department Manager and HR
6.2 Final Warning (FW) - progression from W imposed on the employee for violating the same offense for the second time, or a more serious offense for the first time. It observes the twin-notice rule under the Philippine Labor Code. The employee concerned may be required to be involved in a PIP.	Immediate Superior and noted by the Department Manager and HR
6.3 Suspension (S) -progression from FW and requires the temporary relief of the employee from work on a no-pay status as a penalty for grave offenses or repeated violations. The number of suspension days varies depending upon the violation. It observes both the twin-notice rule under the Philippine Labor Code. The employee concerned may be required to be involved in a PIP. 3 working days 1 week (7 working days) 2 weeks (14 working days) 3 weeks (21 working days)	Immediate Superior, Department Manager, noted by HR
6.4 Preventive Suspension (PS) - The employee shall be placed under PS while a violation is under investigation, whereas, the presence of the employee is a threat to the life, property and/or well-being of the Company or the employees herein. 1 month (30 working days)	Approval by the Incident Response Team and in consultation with the Company's legal counsel
6.5 Dismissal (D) -the employee's termination of employment without any leave benefit. This is an action imposed to an employee who repeatedly violates the same offense, wherein W, FW or S have been previously imposed, and when such offense/s are already of such nature that they establish a just cause or reasonable ground for dismissal under the Philippine Labor Code. It observes the twin-notice rule and a written notice of dismissal shall be served to the concerned employee.	Approval by the Incident Response Team and in consultation with the Company's legal counsel
6.6 Criminal Prosecution ("CP") -Administrative sanctions do not preclude any possible legal action the company may consider.	Approval by the Incident Response Team and in consultation with the Company's legal counsel

MANILA BANKERS
LIFE INSURANCE CORPORATION

3/F VGP Center, 6772 Ayala Avenue, Makati City, 1223 Philippines
www.manilabankerslife.com
customercare@manilabankerslife.com
(632) 810-1040 / 810-1051 / 810-1072/ 815-1004